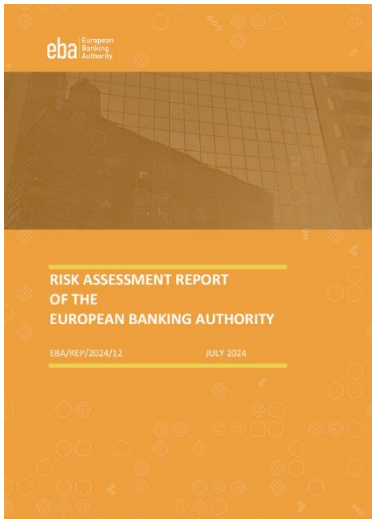
Серійний номер: ДСФМУ-ДК-2024-015
Липень 2024

ЗВІТИ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ та ОКРЕМИХ ЮРИСДИКЦІЙ

Звіт Європейського органу банківського нагляду (EBA) за червень 2024 року: Оцінка ризиків



Звіт Європейського органу банківського нагляду (EBA) за червень 2024 року висвітлює кілька ключових викликів та наслідків для банківського сектора. Банки стикаються зі зростаючою невизначеністю через геополітичні ризики та невизначений економічний прогноз, що вимагає гнучкого планування та оперативних процесів для подолання несподіваних викликів.

- Якість кредитів та активів: Макроекономічні та грошово-кредитні умови уповільнили зростання кредитування. Банки очікують поступового покращення якості активів, але обсяги проблемних кредитів (NPL) серед домашніх господарств і компаній можуть зрости.
- Комерційна нерухомість (CRE): Банки мають значні обсяги кредитів у секторі комерційної нерухомості, деякі з яких вразливі до економічних спадів. Зростання обсягів проблемних кредитів у цьому секторі становить ризик.
- Фінансування та ліквідність: Банки планують збільшити ринкове фінансування, особливо незабезпечене боргове фінансування, щоб замінити застарілі інструменти. Важливість має забезпечення адекватної ліквідності та прийнятних застав, що відповідають вимогам центрального банку.
- Прибутковість: Прибутковість банків, що визначається чистим відсотковим доходом, можливо, досягла піку. Зростаючі витрати на фінансування та можливий тиск на чисті відсоткові маржі вимагають диверсифікованих джерел доходу та ефективного управління витратами.
- Операційний ризик: Ризики кібербезпеки та захисту даних є ключовими проблемами, з огляду на зростаючу кількість кібератак. Санкції та перевірки клієнтів залишаються значними викликами у боротьбі з відмиванням грошей і фінансуванням тероризму.
- Небанківські фінансові посередники (NBFIs): Зростання активності NBFIs у приватному кредитуванні несе можливості та ризики, такі як операційні проблеми та нижчі стандарти кредитування. Потрібні підвищена прозорість та контроль за діяльністю NBFIs.
- Екологічні, соціальні та управлінські (ESG) ризики: Вони стають все більш значущими і вимагають інтеграції у рамки управління ризиками банків. Регулятивні ініціативи забезпечують врахування ESG ризиків як факторів традиційних категорій ризиків.

Банки повинні пріоритетно розглядати управління ризиками, включаючи актуальні оцінки застави та своєчасне резервування кредитів. Вони повинні підтримувати адекватну ліквідність і

диверсифіковані джерела фінансування, стратегічно управляючи ринковим фінансуванням. Важливо обережно управляти виплатами та забезпечити достатні капітальні резерви для поглинання потенційних втрат.

http://surl.li/xvpbmx

Горизонтальний огляд технічної відповідності гейткіперів щодо корупції

Звіт FATF "Horizontal Review of Gatekeepers' Technical Compliance Related to Corruption" аналізує відповідність стандартам FATF серед професіоналів, відомих як "гейткіпери", які включають юристів, бухгалтерів, постачальників трастових послуг та агентів з нерухомості. Основна увага приділяється тому, як ці професіонали можуть несвідомо або свідомо сприяти відмиванню хабарів і незаконно отриманих коштів.

Результати звіту показують, що понад половина членів FATF мають високі показники відповідності, проте деякі важливі вимоги, такі як проведення належної перевірки клієнтів і впровадження внутрішніх контролів, все ще залишаються відстаючими. Багато країн впровадили законодавчі та регуляторні рамки для боротьби з корупцією, але існують значні прогалини в їх практичному застосуванні. Наприклад, деякі професіонали не здійснюють належної перевірки клієнтів або не повідомляють про підозрілі транзакції через недостатню обізнаність або небажання порушувати конфіденційність клієнтів.

FATF також підкреслює важливість впровадження належних внутрішніх політик і процедур для запобігання корупції та відмиванню грошей. Це включає навчання персоналу, оцінку ризиків та впровадження систем внутрішнього контролю. Звіт рекомендує країнам-учасникам підвищити прозорість та підзвітність серед професіоналів, а також посилити нагляд і контроль за їх діяльністю.

Загалом, FATF закликає до посилення міжнародної співпраці та обміну інформацією для ефективної боротьби з корупцією і відмиванням грошей. Професіонали, які працюють у сфері фінансових послуг, мають відігравати ключову роль у забезпеченні дотримання стандартів FATF і запобіганні фінансовим злочинам.

https://bit.ly/3zDiBMP

Звіт AUSTRAC "Національна оцінка ризиків ПВК 2024"

Звіт AUSTRAC "Money Laundering National Risk Assessment (NRA) 2024" аналізує ризики відмивання грошей в Австралії. Цей документ є важливим інструментом для виявлення та розуміння основних загроз та вразливостей, пов'язаних з відмиванням грошей, а також для розробки ефективних стратегій протидії цим загрозам.

Звіт містить детальну оцінку ризиків, пов'язаних з різними секторами економіки, включаючи банківський сектор, фінансові послуги, нерухомість та інші. Він підкреслює, що банки залишаються основною мішенню для відмивання грошей через великий обсяг транзакцій та широку клієнтську базу. Водночас інші сектори, такі як нерухомість і ювелірні вироби, також знаходяться під значним ризиком через можливість здійснення великих готівкових операцій.

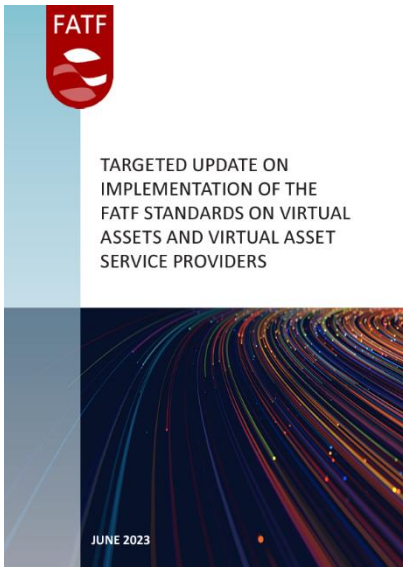
У звіті також розглядаються нові технологічні загрози, пов'язані з криптовалютами та іншими цифровими активами. Ці нові форми фінансових інструментів стають все більш популярними серед злочинців через їхню анонімність та складність відстеження. AUSTRAC закликає до посилення регуляторного контролю над криптовалютними біржами та провайдерами послуг з обміну цифровими активами.

Звіт також підкреслює важливість міжнародної співпраці у боротьбі з відмиванням грошей. Відмивання грошей є глобальною проблемою, яка потребує координованих зусиль з боку різних країн та міжнародних організацій. AUSTRAC наголошує на необхідності обміну інформацією та співпраці з іноземними партнерами для ефективного виявлення та запобігання транснаціональним фінансовим злочинам.

Для підвищення ефективності боротьби з відмиванням грошей AUSTRAC рекомендує розширення навчальних програм для фінансових установ та інших зацікавлених сторін. Це допоможе підвищити обізнаність про ризики та забезпечити належне виконання вимог законодавства.

https://bit.ly/4cRsm8q

Віртуальні активи: Цільове оновлення щодо впровадження стандартів FATF щодо віртуальних активів і постачальників послуг віртуальних активів



Звіт FATF "Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers" аналізує відповідність юрисдикцій стандартам FATF щодо віртуальних активів (VA) та постачальників послуг з віртуальними активами (VASPs).

Основні висновки звіту показують, що більшість юрисдикцій все ще мають труднощі з дотриманням основних вимог, таких як проведення оцінки ризиків, прийняття законодавства для регулювання VASPs та проведення наглядових перевірок. З 98 оцінок взаємного аналізу та подальших звітів FATF, 75% юрисдикцій лише частково або зовсім не відповідають вимогам FATF.

Крім того, прогрес у впровадженні правила Travel Rule, ключового заходу AML/CFT, також є недостатнім. З 151 юрисдикції, що відповіли на опитування FATF у 2023 році, більше половини ще не здійснили жодних кроків щодо впровадження правила Travel Rule, що створює серйозні прогалини для злочинців.

FATF закликає всі країни до швидкого впровадження своїх стандартів на VA та VASPs, включаючи правило Travel Rule. У лютому 2023 року FATF прийняла дорожню карту для покращення впровадження Рекомендації 15. Згідно з цією дорожньою картою, FATF буде продовжувати здійснювати просвітницьку діяльність, надавати допомогу юрисдикціям з низьким рівнем спроможності, публікувати кроки, які вжили юрисдикції-члени FATF та інші важливі юрисдикції, сприяти обміну досвідом та викликами, моніторити ринкові тенденції у цій сфері та проводити подальші огляди прогресу.

https://bit.ly/4cTP2VJ

Пріоритети наглядового органу EBA для емітентів ART/EMT на 2024/2025

Європейський банківський орган (EBA) опублікував чотири ключові пріоритети для нагляду за емітентами активів у формі токенів (ARTs) і електронних грошей (EMTs) на 2024/2025 роки.

Основні сфери уваги включають внутрішнє управління та управління ризиками, фінансову стійкість, управління технологічними ризиками та управління ризиками фінансових злочинів.

Звіт також підкреслює важливість ідентифікації та управління ризиками, пов'язаними з третіми сторонами та аутсорсингом, а також забезпечення дотримання регулятивних вимог. Особливу увагу приділено управлінню технологічними ризиками, включаючи ризики кібербезпеки і ризиків, що виникають внаслідок використання технологій розподіленого реєстру (DLT), а також планам резервного копіювання на випадок порушення роботи цих технологій. Крім того, емітенти ARTs і EMTs повинні забезпечити, щоб особи, які контролюють або керують ART або EMT, мали чисте кримінальне досьє та були перевірені на фінансові злочини.

Звіт також розглядає питання внутрішнього управління та управління ризиками, наголошуючи на необхідності чіткої структури управління з визначеними лініями відповідальності. Для цього потрібне управління з акцентом на відповідні навички та знання в криптосекторі, що включає попередній досвід. Важливим аспектом є забезпечення ефективних та прозорих процедур обробки скарг. Емітенти ARTs і EMTs повинні впроваджувати управління ризиками відповідно до розміру, бізнес-моделей та складності емітентів. Крім того, необхідно ідентифікувати ризики, пов'язані з третіми сторонами, та аутсорсингом з акцентом на управління ризиками кастодіальних операцій.

Забезпечення повної відповідності власним вимогам та вимогам щодо складу активів є ключовим пріоритетом для емітентів. Вони повинні мати якісні резерви активів, щоб відповідати вимогам MiCA, а також ідентифікувати загрози кіберризиків. Емітенти мають описати критерії вибору використовуваних технологій розподіленого реєстру (DLT) та мати плани резервного копіювання у разі порушення роботи цих технологій.

Ці пріоритети наголошують на необхідності емітентів ART і EMT бути готовими до нових регулятивних вимог і забезпечити дотримання високих стандартів у своїй діяльності.

http://surl.li/fhqpek

Національна стратегія Сінгапуру з протидії фінансуванню тероризму

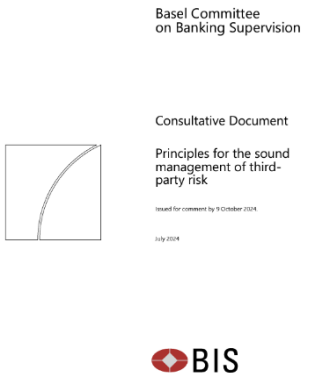
Сінгапур оновив свою Національну стратегію з протидії фінансуванню тероризму, базуючись на нещодавно опублікованій Національній оцінці ризиків фінансування тероризму (TF NRA). Ключові моменти включають визначення найбільших загроз, таких як радикалізовані індивіди, вплив глобальних та регіональних подій.

Найбільший ризик представляють грошові перекази, особливо нелегальні та міжнародні онлайн-платежі. Банківський сектор залишається на середньо-високому рівні ризику, але жодна система банківських або міжнародних швидких платежів не була використана для фінансування тероризму.

Провайдери цифрових платіжних токенів збільшили свій ризик з середньо-низького в 2020 році до середньо-високого в 2024 році, незважаючи на відсутність доказів використання віртуальних активів для фінансування тероризму. Зловживання неприбутковими організаціями, перетин кордонів з готівкою та операції з дорогоцінними каменями та металами залишаються на середньо-низькому рівні ризику.

http://surl.li/cbyeip

Принципи надійного управління ризиками третіх сторін



Базельський комітет з банківського нагляду (BCBS) опублікував консультативний документ, який пропонує принципи для ефективного управління ризиками, пов'язаними з третіми сторонами, в банківському секторі. Документ наголошує на важливості розробки чітких політик і процедур для оцінки, моніторингу та управління ризиками, що виникають у зв'язку з використанням сторонніх постачальників послуг. Це включає встановлення належного процесу вибору та належної перевірки постачальників, постійного моніторингу їхньої діяльності, а також забезпечення надійного управління контрактами та відповідності нормативним вимогам.

Документ також підкреслює необхідність чіткого розподілу відповідальності в рамках організації, щоб забезпечити ефективне управління третіми сторонами. Важливо, щоб банки мали можливість адаптувати свої підходи до управління ризиками в залежності від масштабу і складності своїх операцій та рівня ризиків, пов'язаних з конкретними постачальниками. Враховуючи зростаючу цифровізацію та швидкий розвиток фінансових технологій, ці принципи забезпечують гнучкість для адаптації до змінюваних практик та нормативних рамок у різних юрисдикціях.

Документ закликає банки до постійного вдосконалення своїх підходів до управління ризиками, враховуючи нові загрози та виклики, що виникають у зв'язку з використанням сторонніх постачальників послуг. Він також підкреслює важливість співпраці з наглядовими органами для забезпечення належного контролю та підтримки високих стандартів управління ризиками.

https://www.bis.org/bcbs/publ/d577.pdf

Оглядовий документ щодо децентралізованих автономних організацій

Law Commission
Reforming the law

Комісія з права Англії та Уельсу опублікувала оглядовий документ, що аналізує правові аспекти Децентралізованих Автономних Організацій (DAO). DAO – це новий тип організацій, які використовують розподілені реєстри та смарт-контракти для управління без централізованого контролю. Вони діють за

допомогою правил, прописаних у комп'ютерному коді, і можуть функціонувати автономно, приймаючи рішення на основі алгоритмів та голосування учасників. Цей документ досліджує різні правові питання, пов'язані з DAO, включаючи їх правовий статус, відповідальність учасників, регуляторні виклики та потенційні ризики.

Один з ключових аспектів документу – це аналіз правової кваліфікації DAO. Комісія вивчає, чи можуть DAO бути визнані юридичними особами, і які наслідки це матиме для їхньої діяльності та учасників. Також розглядається питання відповідальності учасників DAO, оскільки відсутність централізованого контролю може ускладнювати визначення відповідальних осіб у разі порушень або збитків. Регуляторні виклики також займають значне місце в аналізі, зокрема питання, як існуючі правові рамки можуть бути адаптовані для включення DAO, і чи потребують вони спеціальних нормативних актів.

Комісія також аналізує можливі зміни до Закону про компанії 2006 року та регуляцій щодо боротьби з відмиванням грошей для забезпечення більшої сумісності з технологіями розподіленого реєстру. Вони рекомендують уряду продовжувати моніторинг розвитку DAO та бути готовими до потенційних змін у законодавстві. Документ також підкреслює важливість міжнародної співпраці у врегулюванні правових питань, пов'язаних з DAO, оскільки ці організації часто діють у глобальному масштабі.

http://surl.li/fhisfz

РЕГУЛЮВАННЯ

ЄС розширює сферу дії санкцій проти Білорусі для боротьби з обходом санкцій

Європейська Комісія оголосила про новий пакет санкцій проти Білорусі, посилюючи заходи для запобігання обходу санкцій, спрямованих на Росію. Санкції включають обмеження на експорт товарів подвійного призначення та передових технологій, заборону на імпорт золота і діамантів з Білорусі, а також обмеження на надання транспортних і фінансових послуг білоруськими компаніями.

Санкції відображають зростаючу стурбованість ЄС щодо ролі Білорусі в підтримці агресії Росії проти України. ЄС продовжує працювати над тим, щоб перекрити всі можливі шляхи обходу санкцій, використовуючи нові законодавчі інструменти та посилюючи міжнародне співробітництво. Зокрема, посилено контроль за експортом товарів, які можуть бути використані для військових цілей, що сприяє зниженню можливостей для білоруських компаній обходити санкції через посередників та інші країни.

Нові санкції також включають додаткові заходи щодо фінансових обмежень, спрямованих на білоруські банки та фінансові установи, що посилює економічний тиск на режим Лукашенка. Європейська Комісія заявила, що ці санкції є необхідними для підтримки тиску на Білорусь з метою припинення її участі у військових діях Росії та порушень міжнародного права. ЄС також закликає інші країни приєднатися до санкційного режиму, щоб забезпечити ефективність міжнародних зусиль у боротьбі з обходом санкцій.

https://bit.ly/3WeXhGm

Звіт "Global REG-CAP" за червень 2024 року від FINTRAIL

Звіт "Global REG-CAP" за червень 2024 року, підготовлений FINTRAIL, підсумовує зміни в регулюванні фінансових злочинів та публікації за останній місяць. Основні моменти включають оновлення від FATF, де Ямайка та Туреччина були виключені зі списку підвищеного моніторингу, а Монако та Венесуела додані до нього. FATF також оновлює свої рекомендації щодо національних оцінок ризиків. ЄС погодив новий пакет санкцій проти Росії, який вперше торкнеться постачання зрідженого природного газу. FCA відклала оприлюднення огляду щодо внутрішніх політично значущих осіб до липня. Глобальна коаліція з боротьби з фінансовими злочинами опублікувала звіт про фінансові шахрайства в Східній Азії.

https://fintrail.com/regcap-content/2024/7/8/global-reg-cap-june-2024

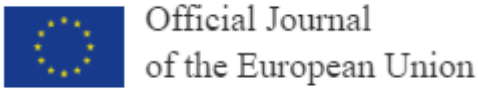
FinCEN про модернізацію програм AML/CFT

FinCEN запропонувала нові правила для модернізації та посилення програм з протидії відмиванню грошей (AML) та фінансуванню тероризму (CFT) у фінансових установах. Зміни передбачають обов'язковий процес оцінки ризиків і врахування загальнонаціональних пріоритетів AML/CFT, спрямовані на створення ефективних ризик-орієнтованих програм. Фінансові установи заохочуються до модернізації своїх програм та впровадження інновацій, при цьому керуючи ризиками нелегальних фінансів. Нові правила спрямовані на уникнення підходу "один розмір підходить всім" та надання більшої гнучкості установам.

Пропоновані зміни до чинних правил підкреслюють необхідність адаптації програм AML/CFT до специфічних ризиків, з якими стикаються фінансові установи. FinCEN прагне забезпечити, щоб ці програми були не лише формальними, але й ефективними у виявленні та запобіганні фінансовим злочинам. Важливим елементом є також співпраця з іншими регуляторами та зацікавленими сторонами для досягнення загальнонаціональних цілей у сфері AML/CFT. Це включає обмін інформацією та кращими практиками, що дозволить фінансовим установам більш ефективно боротися з загрозами відмивання грошей та фінансування тероризму.

http://surl.li/othicb

Регламент (ЄС) 2024/1624 від 31 травня 2024 року



Регламент (ЄС) 2024/1624 Європейського Парламенту та Ради від 31 травня 2024 року спрямований на запобігання використанню фінансової системи для відмивання грошей та фінансування тероризму. Документ встановлює обов'язкову оцінку ризиків для фінансових установ, впровадження внутрішніх політик, процедур і контролю для забезпечення дотримання вимог боротьби з відмиванням грошей (AML) та фінансуванням тероризму (CFT). Фінансові установи повинні впровадити належні заходи щодо перевірки клієнтів (CDD), включаючи ідентифікацію та перевірку особи клієнтів і кінцевих бенефіціарних власників, моніторинг транзакцій та повідомлення про підозрілі дії.

Регламент також передбачає обов'язкове зберігання записів, обробку персональних даних і обмін інформацією між фінансовими установами та наглядовими органами. Це включає обов'язок повідомляти фінансові розвідувальні підрозділи (FIUs) про підозрілі транзакції, співпрацювати з Європейською прокуратурою (EPPO) та іншими міжнародними організаціями. Важливою частиною регламенту є заходи щодо обмеження анонімних рахунків та великих готівкових платежів. Зокрема, регламент забороняє відкриття анонімних банківських рахунків та встановлює обмеження на великі готівкові операції для запобігання фінансовим злочинам.

Додатково, регламент визначає обов'язки трастів, номінантів і іноземних юридичних осіб у контексті прозорості власності та контролю. Він зобов'язує ці суб'єкти забезпечувати належну ідентифікацію бенефіціарних власників та повідомляти про будь-які зміни у власності чи контролі.

https://eur-lex.europa.eu/eli/reg/2024/1624/oj

ЗВІТИ ОКРЕМИХ КОМПАНІЙ та ЕКСПЕРТІВ

Ризики боротьби з відмиванням коштів (AML) і протидії фінансуванню тероризму (CTF)

Дослідження Arctic Intelligence аналізує ризики, пов'язані з відмиванням грошей (AML) та фінансуванням тероризму (CTF). Воно підкреслює важливість дотримання законів AML/CTF для захисту глобальної економіки та безпеки. Дослідження пояснює, що відмивання грошей передбачає легалізацію незаконно отриманих коштів через складні фінансові транзакції, тоді як фінансування тероризму полягає у наданні фінансових ресурсів для підтримки терористичної діяльності.

Ризики AML/CTF виникають через можливість використання легітимних фінансових систем для легалізації злочинних доходів або фінансування тероризму. Для оцінки цих ризиків проводяться систематичні аналізи, що включають вивчення клієнтських профілів, транзакційних моделей, географічних місць та характеристик продуктів і послуг. Метою таких оцінок є розробка стратегій та заходів для ефективного зниження ризиків та забезпечення відповідності законодавчим вимогам.

сновні ризики, розглянуті в статті:

- Ризики середовища: Вразливість організації до ризиків відмивання грошей і фінансування тероризму через зовнішнє та внутрішнє середовище.
- Бізнес-ризики: Ризики, пов'язані з операційною діяльністю організації, включаючи локацію бізнесу та ризики аутсорсингу.
- Клієнтські ризики: Ризики, пов'язані з клієнтами, які можуть бути залучені до відмивання грошей або фінансування тероризму.
- Ризики продуктів і послуг: Ризики, пов'язані з характеристиками продуктів та послуг, які можуть бути привабливими для злочинців.
- Канальні ризики: Ризики, пов'язані з різними способами доступу до продуктів і послуг.
- Транзакційні ризики: Ризики, пов'язані з типами транзакцій, включаючи обсяги та частоту транзакцій.
- Географічні ризики: Ризики, пов'язані з географічним розташуванням бізнесу або клієнтів.

Проведення оцінки ризиків AML/CTF допомагає організаціям ідентифікувати та аналізувати потенційні ризики, розробляти відповідні стратегії для їх зниження та забезпечувати дотримання законодавства. Це також сприяє підтриманню репутації компанії, фінансовій безпеці та ефективному виявленню та запобіганню фінансовим злочинам.

https://fincrimeagent.com/aml-and-financial-crime-policies-and-procedures/

Оцінка шахрайства у Східній Азії

Звіт "An Assessment of Scams in East Asia" від Глобальної коаліції з боротьби з фінансовими злочинами аналізує масштаби шахрайства в Східній Азії, зосереджуючи увагу на Австралії, Гонконзі та Сінгапурі. У звіті виділено понад 20 основних видів шахрайства, серед яких є гібридні форми злочинної діяльності, що призводять до значних фінансових втрат, зміни способу життя та навіть самогубств. Серед найбільш розповсюджених видів шахрайства є фінансові піраміди, фішинг, шантаж через онлайн-платформи та інвестиційні шахрайства.

Оцінюючи втрати від шахрайства, звіт підкреслює, що якщо екстраполювати ці дані на глобальний рівень, втрати можуть становити від 50 до 177 мільярдів доларів США. Причини, що роблять ці країни привабливими для шахраїв, включають високе економічне багатство, високий рівень цифровізації та обмежену обізнаність громадян про шахрайські схеми. Шахраї використовують технологічні досягнення для створення все більш складних схем, які важко виявити та зупинити.

Звіт також підкреслює важливість підвищення обізнаності населення та вдосконалення регуляторних заходів для боротьби з шахрайством. Рекомендації включають розширення освітніх програм для громадян, посилення міжнародної співпраці та впровадження нових технологій для виявлення та запобігання шахрайству.

https://www.gcffc.org/an-assessment-of-scams-in-east-asia/

Індія – зростає занепокоєння з приводу зловживання стандартами FATF проти громадянського суспільства

Звіт Amnesty International та Front Line Defenders висловлює серйозні занепокоєння щодо зловживання законами про боротьбу з тероризмом в Індії для цілеспрямованих нападів на представників громадянського суспільства.

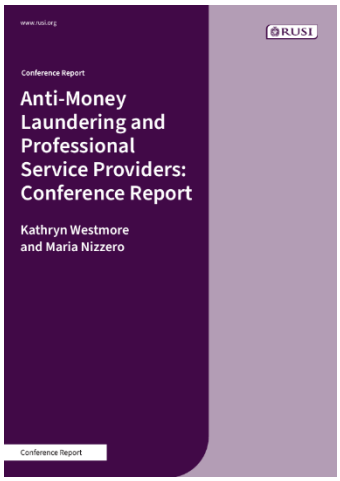
Напередодні шостого пленарного засідання Групи з фінансових заходів боротьби з відмиванням грошей (FATF), де буде переглядатися Звіт про взаємну оцінку Індії, автори звіту закликають членів FATF врахувати занепокоєння громадянського суспільства і нагадати уряду Індії про їхні зобов'язання дотримуватися рекомендацій FATF без зловживань. У звіті підкреслюється, що поточні дії уряду Індії порушують стандарти FATF і права громадянського суспільства, особливо щодо свободи вираження думок і зібрань.

Зокрема, звіт вказує на те, що уряд Індії використовує закони про боротьбу з тероризмом для переслідування активістів, журналістів та інших представників громадянського суспільства. Вони піддаються арештам, переслідуванням та обмеженням, що порушує їхні основні права. Amnesty International закликає FATF звернути увагу на ці зловживання під час оцінки Індії та закликати уряд Індії дотримуватися міжнародних стандартів прав людини.

У звіті також зазначено, що Індія повинна припинити практику переслідування громадянського суспільства та забезпечити належне впровадження рекомендацій FATF без порушення прав людини. Організації закликають FATF посилити моніторинг дій уряду Індії та вжити заходів для запобігання подальшим порушенням. Це включає в себе забезпечення прозорості процесів, захист прав активістів та гарантування свободи слова та зібрань.

https://www.amnesty.org/en/documents/asa20/8202/2024/en/

Боротьба з відмиванням коштів та професійні постачальники послуг



Звіт "Anti-Money Laundering and Professional Service Providers: Conference Report" авторів Кетрін Вестмор і Марії Ніццеро обговорює питання підвищення ефективності нагляду за юристами та бухгалтерами у Великобританії та ЄС.

Основні питання включають використання стимулів і санкцій для забезпечення дотримання правил та стратегії для покращення співпраці. Звіт базується на даних останнього звіту Групи фінансових заходів боротьби з відмиванням грошей (FATF), який показує, що понад половина членів FATF, включаючи Великобританію та багато європейських країн, досягли понад 80% технічної відповідності для професійних гейткіперів. Проте ефективність залишається питанням, яке потребує подальшого розгляду.

Звіт підсумовує висновки, отримані на семінарах, організованих у партнерстві з Делегацією ЄС у Великобританії, та зосереджується на трьох елементах: виклики, які перешкоджають ефективності нагляду у Великобританії та ЄС, і шляхи їх подолання; інструменти правозастосування та способи підтримки співпраці через кордони; стимули, які можуть заохотити професійних постачальників послуг діяти як ефективні гейткіпери.

Автори звіту зазначають, що підвищення ефективності нагляду за юристами та бухгалтерами є важливим кроком для боротьби з відмиванням грошей та фінансуванням тероризму. Використання стимулів та санкцій може сприяти забезпеченню дотримання правил, а також підвищити рівень співпраці між різними юрисдикціями. Зокрема, важливо забезпечити, щоб професійні постачальники послуг, такі як юристи та бухгалтери, діяли як ефективні гейткіпери, запобігаючи використанню своїх послуг для відмивання грошей.

Одним із ключових аспектів є використання інструментів правозастосування, що можуть допомогти у виявленні та розслідуванні випадків відмивання грошей. Крім того, важливо забезпечити ефективну співпрацю між різними юрисдикціями, що дозволить обмінюватися інформацією та координувати зусилля у боротьбі з фінансовими злочинами. Стимули для професійних постачальників послуг можуть включати як позитивні, так і негативні аспекти, такі як фінансові винагороди за дотримання правил або штрафи за їх порушення.

Звіт підкреслює важливість створення сприятливих умов для професійних постачальників послуг, що дозволить їм ефективно виконувати свої функції як гейткіперів. Для досягнення цього необхідно забезпечити належну підготовку та освіту, а також доступ до необхідних ресурсів та інструментів. Крім того, важливо забезпечити, щоб регуляторні органи мали достатні повноваження та ресурси для здійснення нагляду та правозастосування.

http://surl.li/bspjxh

Прихована валюта: державні та недержавні особи у фінансуванні шпигунства

Стаття від Insight Monitor розглядає фінансування шпигунства, зокрема методи, які використовуються державними та недержавними особами для збору та передання секретної інформації. Фінансування шпигунства включає виплати грошима за секретну інформацію, використання технологій для передачі коштів і способи підготовки агентів. Основними джерелами фінансування є державні бюджети, посольства, електронні перекази та готівка, хоча все частіше використовуються криптовалюти. Стаття наводить приклади з Канади, США та інших країн, демонструючи різноманітність методів і масштабів виплат шпигунам.

Описуються випадки з Канади, як-от справа Камерона Ортіса та Джеффрі Деліля, а також випадки з США, включаючи дії екс-агентів ЦРУ та ФБР. Виплати шпигунам часто варіюються від кількох десятків тисяч до мільйонів доларів. Використання криптовалют, таких як Monero, стає популярним завдяки їхній анонімності та безпеці. Проте готівка залишається основним способом оплати, особливо для шпигунів і агентів, щоб зберегти анонімність і уникнути відстеження.

Фінансування шпигунської діяльності також може здійснюватися через комерційні структури, наприклад, у випадку з Danske Bank, що стала об'єктом розслідування через підозри у відмиванні грошей. У звіті також наводяться приклади з Австралії та Зімбабве, де шпигунська діяльність фінансується через комерційні підприємства.

Виявлення фінансування шпигунства є складним завданням, яке потребує спільних зусиль правоохоронних органів, фінансових установ та міжнародної спільноти.

https://newsletter.insightthreatintel.com/p/espionage-financing

MiCAR тепер застосується до токенів прив'язаних до активів та токенів електронних грошей

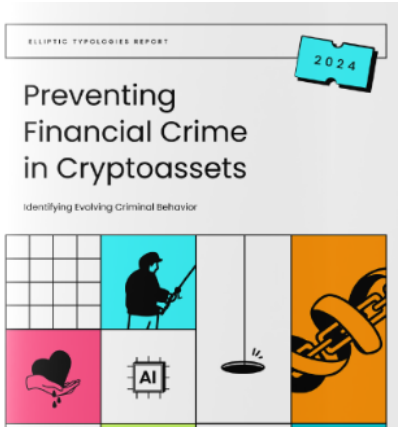
Європейський регламент "Markets in Crypto-Assets Regulation" (MiCAR) тепер застосовується до токенів, прив'язаних до активів (ART), та електронних грошових токенів (EMT). З 30 червня 2024 року Titles III та IV MiCAR набули чинності, зосереджуючись на ART та EMT. ART – це стейблкоіни, що підтримують стабільну вартість відносно офіційних валют або інших активів. Вони надають стабільність та забезпечення для інвесторів, що дозволяє зменшити волатильність криптовалютного ринку. EMT пов'язані з однією офіційною валютою та діють як електронні гроші. Вони надають можливість здійснювати транзакції з використанням цифрових активів, що мають стабільну вартість, подібно до традиційних грошей.

Для пропозиції ART потрібна авторизація, подібна до PSD2 та EMD2, а також white paper, схвалена регулятором. Ця процедура гарантує, що компанії, які випускають ART, дотримуються суворих правил і забезпечують прозорість своєї діяльності. EMT можуть випускатися лише кредитними установами або установами-емітентами електронних грошей, з обов'язковим інвестуванням у безпечні активи та планом відновлення та викупу. Це гарантує, що EMT підтримуються надійними фінансовими інститутами та забезпечують безпеку для користувачів.

Нові вимоги MiCAR також включають заходи щодо захисту інвесторів та користувачів, а також вимоги до управління ризиками та прозорості. Вони спрямовані на запобігання зловживанням та забезпечення стабільності на ринку криптоактивів. Ці заходи включають обов'язкове розкриття інформації, вимоги до звітності та аудиту, а також вимоги до капіталу для забезпечення фінансової стійкості компаній, що випускають ART та EMT.

http://surl.li/wvlxmh

Запобігання фінансовим злочинам у криптоактивах: виявлення еволюції злочинної поведінки



Звіт Elliptic " Preventing Financial Crime in Cryptoassets: Identifying Evolving Criminal Behavior 2024" розкриває деталі еволюції та поточних тенденцій у сфері криптовалютних фінансових злочинів.

Документ надає глибокий аналіз змін в інтеграції криптоактивів із злочинною діяльністю, висвітлюючи нові типології та схеми, які використовуються зловмисниками. Основні акценти зроблено на зближенні штучного інтелекту (ШІ) та криптовалют, що відкриває нові можливості для злочинців, а також на зростаючій ролі стейблкоінів у схемах шахрайства та ухиляння від санкцій. Важливі кейси демонструють практичні приклади використання блокчейн-аналітики для виявлення та протидії таким схемам.

Один із ключових розділів звіту присвячений використанню штучного інтелекту в злочинних операціях із криптовалютами. Злочинці дедалі частіше використовують ШІ для автоматизації своїх дій, включаючи відмивання грошей та фінансові махінації. Це ускладнює роботу правоохоронних органів та підрозділів боротьби з фінансовими злочинами, оскільки традиційні методи виявлення та протидії стають менш ефективними. Звіт також підкреслює важливість використання сучасних технологій та інструментів блокчейн-аналітики для ефективного виявлення нових типологій фінансових злочинів.

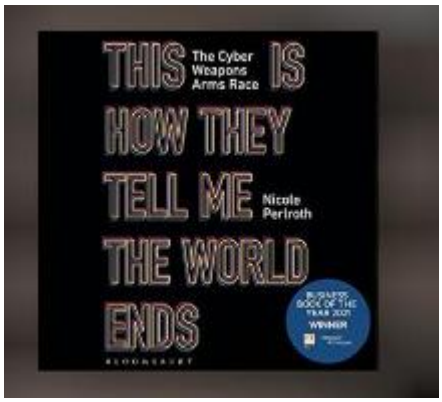
Ще одним значущим аспектом є зростання використання стейблкоінів у злочинних схемах. Стейблкоіни, прив'язані до фіатних валют, забезпечують зловмисникам більшу стабільність та меншу волатильність, що робить їх привабливими для відмивання грошей та інших фінансових злочинів. Звіт описує конкретні схеми, такі як "pig butchering", де стейблкоіни використовуються для приховування незаконних операцій.

Звіт також містить рекомендації для фінансових установ і правоохоронних органів щодо підвищення ефективності протидії фінансовим злочинам. Це включає в себе використання новітніх технологій, посилення міжнародної співпраці та вдосконалення нормативної бази для забезпечення більшої прозорості та безпеки у сфері криптоактивів.

https://www.elliptic.co/resources/elliptic-typologies-report-2024

РЕКОМЕНДОВАНІ МАТЕРІАЛИ

"This Is How They Tell Me the World Ends" Ніколь Перлрот



Книга "This Is How They Tell Me the World Ends" написана Ніколь Перлрот, журналісткою New York Times, яка спеціалізується на кібербезпеці і цифрових загрозах.

Ця книга є глибоким дослідженням кібербезпеки та глобальних загроз, пов'язаних з кіберпростором, яка поєднує аналітику, журналістські розслідування та особисті інтерв'ю. У книзі розкривається історія виникнення та еволюції кіберзброї, починаючи з перших вірусів і закінчуючи сучасними складними атаками, описується, як уряди та приватні компанії розробляють, купують і використовують кіберзброю для своїх цілей. Перлрот детально розповідає про існування підпільного ринку, де продаються та купуються вразливості в програмному забезпеченні, що можуть бути використані для кібератак, і пояснює, як ці ринки функціонують і як вони впливають на глобальну безпеку.

В книзі аналізуються відомі кібернапади, такі як атаки на Sony Pictures, WannaCry, NotPetya, та інші, де описуються не тільки технічні аспекти атак, але й їхні політичні та економічні наслідки. Розглядається роль урядів в регулюванні кіберпростору та боротьбі з кіберзагрозами, обговорюються міжнародні угоди, які намагаються встановити правила для кіберпростору, але стикаються з труднощами через відмінності в підходах різних країн.

Авторка включає численні інтерв'ю з експертами з кібербезпеки, хакерами, представниками урядів та бізнесу, які допомагають краще зрозуміти мотивації та дії різних гравців на кіберсцені. Перлрот підкреслює, що кіберзагрози продовжують зростати, стають все більш складними та руйнівними, і вказує на те, що багато урядів та організацій не готові до належного захисту від кібератак, що залишає їх вразливими. Вона закликає до більшої міжнародної співпраці та створення ефективних регулюючих механізмів для протидії кіберзагрозам.

"This Is How They Tell Me the World Ends" є важливою працею для розуміння сучасних викликів у сфері кібербезпеки, яка не лише інформує про технічні аспекти кібератак, але й надає глибокий аналіз політичних, економічних та соціальних наслідків цих загроз. Книга є корисною як для фахівців у сфері кібербезпеки, так і для широкої аудиторії, що цікавиться сучасними глобальними проблемами.

http://surl.li/jahblc

ІНШІ НОВИНИ

Відповідність криптобірж правилам Travel Rule ЄС в 2024 році

Стаття на Cointelegraph аналізує нові правила ЄС щодо криптовалютних бірж, які набувають чинності 30 грудня 2024 року. Ці правила, відомі як Travel Rule, спрямовані на посилення заходів проти відмивання грошей (AML) і фінансування тероризму (CFT) для криптовалютних бірж і постачальників послуг з криптоактивами (CASP) у Європейському Союзі.

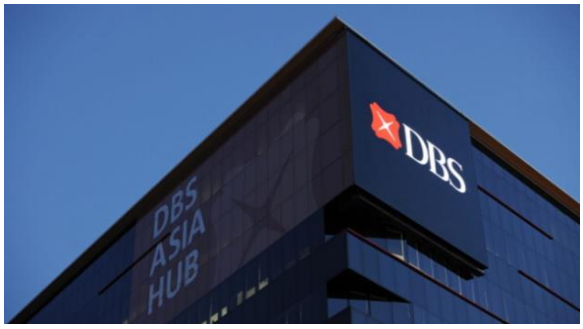
Згідно з новими правилами, криптовалютні біржі повинні збирати та передавати інформацію про відправника і отримувача коштів у транзакціях, що перевищують певний поріг. Це включає ім'я, адресу гаманця, фізичну адресу або інший ідентифікаційний номер. Travel Rule передбачає заходи для запобігання використанню криптовалют для анонімних і незаконних транзакцій, вимагаючи від VASP здійснювати належну перевірку клієнтів та забезпечувати захист переданих даних від кіберзлочинців.

FATF (Група з розробки фінансових заходів боротьби з відмиванням грошей) рекомендує усім своїм членам прийняти Travel Rule для боротьби з глобальними загрозами відмивання грошей і фінансування тероризму.

Криптовалютні біржі в ЄС матимуть двомісячний перехідний період після впровадження нових правил для забезпечення відповідності, що надає їм час на адаптацію систем і процесів до нових вимог. Дотримання нових правил вимагатиме значних інвестицій у технології та системи для збору та захисту даних, але довгострокові вигоди від посиленої безпеки та зниження ризиків відмивання грошей переважують витрати. Нові вимоги сприятимуть більшій прозорості у криптовалютних транзакціях, що допоможе у виявленні та запобіганні незаконних фінансових операцій, але також означатиме, що користувачі криптовалют повинні будуть надавати більше особистої інформації, що може підвищити ризики, пов'язані з конфіденційністю даних.

https://bit.ly/4f0ZJYg

Штраф DBS Bank Hong Kong



Гонконзький регуляторний орган (HKMA) наклав штраф у розмірі 10 мільйонів HKD на DBS Bank (Hong Kong) Limited (DBSHK) за недотримання вимог протидії відмиванню грошей (AML) та фінансуванню тероризму (CFT). Розслідування HKMA, яке охоплювало період з 2012 по 2019 рік, виявило кілька серйозних порушень.

По-перше, DBSHK не змогла отримати та перевірити документи, що посвідчують особу, для 60% клієнтів-юридичних осіб, залучених до процесу відкриття рахунків. Це призвело до значного ризику відмивання грошей. По-друге, банк проводив неповні процедури належної перевірки клієнтів (CDD), що включало неактуальну та недоречну інформацію. Зокрема, з жовтня 2017 року по квітень 2019 року банк не проводив перевірок для 23 клієнтів, що значно підвищувало ризик.

Крім того, між березнем та вереснем 2017 року банк не зміг виявити та розслідувати підозрілі транзакції, які не мали очевидних економічних або законних цілей для 15 клієнтів, що означає серйозні прогалини в моніторингу транзакцій. У період з грудня 2018 по лютий 2019 року DBSHK не вжив достатніх заходів для визначення джерела багатства та коштів високоризикових клієнтів, що призвело до невиконання вимог щодо мінімізації ризиків відмивання грошей.

Протягом усього періоду розслідування банк мав дефіцит ефективних внутрішніх процедур для моніторингу бізнес-відносин, проведення комплексних CDD-перевірок та перевірки ідентифікаційних документів. Це підкреслює серйозні недоліки в управлінні ризиками та внутрішньому контролі.

Рішення НКМА про накладення штрафу підкреслює зобов'язання регулятора забезпечувати суворе дотримання норм AML/CFT. Це служить важливим нагадуванням для фінансових установ про необхідність постійного моніторингу та вдосконалення своїх програм відповідності. НКМА наголосив на важливості невідкладного реагування та усунення виявлених недоліків, щоб запобігти подібним випадкам у майбутньому.

Ця дисциплінарна дія є чітким сигналом для індустрії про те, що недотримання норм не буде толеруватися, і що фінансові установи повинні пріоритетно вдосконалювати свої внутрішні механізми контролю для ефективної боротьби з фінансовими злочинами.

https://bit.ly/3Yhtrmb

Справа Магнітського: Як Швейцарія не розслідувала російські мільйони

Стаття "Magnitsky Case: When Russian Millions Go Uninvestigated in Switzerland" аналізує ситуацію навколо нерозслідуваних мільйонів доларів, пов'язаних зі справою Магнітського в Швейцарії. Незважаючи на заморожування 18 мільйонів швейцарських франків на рахунках трьох російських громадян, швейцарська прокуратура вирішила повернути 14 мільйонів з цих коштів, заявляючи про відсутність доказів для висунення обвинувачень. Таке рішення викликало критику, адже тільки частина заморожених коштів була конфіскована, а решта повернута власникам.

Сергій Магнітський, російський юрист і аудитор, розкрив масштабну корупційну схему в Росії, що призвело до його арешту і смерті у в'язниці в 2009 році. Його справа стала символом боротьби проти корупції та порушень прав людини. У відповідь на його смерть міжнародна спільнота, включаючи США, прийняла "Акт Магнітського", який накладає санкції на російських чиновників, причетних до порушень прав людини. Швейцарія, незважаючи на заморожування рахунків, зіткнулася з критикою за недбале розслідування і повернення більшої частини коштів.

Стаття піднімає питання про ефективність швейцарської правової системи у боротьбі з міжнародною корупцією та фінансовими злочинами. Вона також підкреслює вплив міжнародних санкцій на боротьбу з корупцією і необхідність більш рішучих дій з боку швейцарської влади для захисту правосуддя. Повернення більшої частини заморожених коштів викликає сумніви щодо зобов'язань Швейцарії у боротьбі з фінансовими злочинами і забезпеченні правосуддя для жертв корупції.

https://bit.ly/3XUySHr

Узбекистанця екстрадували з України та звинувачують у крадіжці мільйонів доларів у криптовалюті

Нікіта Андрійович Склюєв, громадянин Узбекистану, був екстрадований з України до США та звинувачений у масштабній крадіжці криптовалюти.

У червні 2018 року Склюєв завантажив програму "EOSIO Wallet Explorer" до Apple App Store, яка насправді була шкідливою і призначалася для крадіжки приватних ключів користувачів криптогаманців. Один користувач з Нью-Йорка встановив цю програму і втратив доступ до свого криптогаманця, в якому зберігалось 2,092,395.5356 EOS, що еквівалентно $11.8 мільйонам.

Після крадіжки Склюєв перевів викрадені кошти на свої криптоаккаунти і використав їх для особистих потреб. Це включало покупку люксових товарів, оплату послуг та інші витрати. Завдяки зусиллям правоохоронних органів США, Румунії та України, Склюєв був арештований у Румунії, а пізніше екстрадований до США для пред'явлення звинувачень. Йому загрожує до 20 років ув'язнення за крадіжку криптовалюти та інші пов'язані злочини.

Цей випадок підкреслює важливість міжнародної співпраці у боротьбі з кіберзлочинами та показує, як злочинці використовують новітні технології для здійснення фінансових злочинів. Склюєв буде відповідати за свої дії перед американським судом, що стане попередженням для інших потенційних злочинців у сфері криптовалюти.

https://bit.ly/3RZ0I1u

Франція: EPPO розслідує митне шахрайство з окулярами, імпортованими з Китаю

Європейська прокуратура (EPPO) розслідує масштабне митне шахрайство, пов'язане з імпортом окулярів з Китаю до країн ЄС. Виявлено, що окуляри, виготовлені за низькою ціною в Китаї, продавалися через інтернет за заниженими цінами для уникнення сплати митних зборів і податків.

Це шахрайство призвело до значних фінансових втрат для ЄС і несправедливої конкуренції на ринку. Спільні обшуки в Бельгії, Франції та Нідерландах залучили 90 правоохоронців, які провели обшуки у 17 місцях і допитали 25 осіб.

Розслідування показало, що компанії використовували фальшиві інвойси та інші документи для заниження вартості товарів, щоб знизити митні платежі. В результаті цього, митні органи недоотримали значні суми, а конкуренція на ринку була спотворена через нижчі ціни на нелегально ввезені товари.

Розслідування також виявило мережу підставних компаній, створених для приховування кінцевих бенефіціарів та уникнення відповідальності. Ці компанії діяли у кількох країнах, що ускладнювало відстеження незаконних операцій. Під час обшуків правоохоронці вилучили велику кількість документів і цифрових доказів, які підтверджують факти шахрайства. Крім того, були заморожені банківські рахунки та активи підозрюваних компаній, щоб запобігти подальшому виведенню коштів.

EPPO закликає до посилення міжнародної співпраці для ефективної боротьби з митними шахрайствами і підвищення обізнаності про такі злочини серед громадськості та бізнесу. Це розслідування підкреслює важливість координації зусиль між різними країнами ЄС для захисту економічних інтересів та забезпечення справедливості на ринку.

https://bit.ly/3VTwKwS

Використання підроблених торгових документів у схемах відмивання грошей в ОАЕ

У 2022 і 2023 роках органи ОАЕ отримали кілька сотень повідомлень про відмивання грошей, заснованих на торгівлі (TBML), де широко використовувалися підроблені торгові документи та фіктивні вантажі для приховування руху незаконних коштів. У більшості випадків маніпуляції документами включали зміну дат відправлення, портів навантаження та контейнерних номерів, що становило 41% всіх випадків TBML. У 61% випадків використовувалися фіктивні вантажі, де, незважаючи на наявність документів і фактичних платежів, товари ніколи не відправлялися.

Ці шахрайські схеми дозволяли злочинцям переводити значні суми грошей через міжнародні торгові угоди, уникаючи уваги регуляторів. Влада ОАЕ вжила заходів для посилення моніторингу та розслідування таких випадків, зокрема посилення співпраці з міжнародними партнерами та впровадження нових технологій для виявлення підроблених документів і фіктивних транзакцій. Це розслідування підкреслює важливість прозорості та ретельного контролю у міжнародній торгівлі для запобігання фінансовим злочинам.

http://surl.li/zuvhzx

ДЛЯ ЗАГАЛЬНОГО РОЗВИТКУ

Політика та процедури боротьби з відмиванням коштів та фінансовими злочинами

Дослідження аналізує важливість політик і процедур у боротьбі з відмиванням грошей (AML) та фінансовими злочинами. Політики визначають основні принципи та стратегічні напрямки організацій у боротьбі з фінансовими злочинами, встановлюючи основи для прийняття рішень і дій. Процедури конкретизують ці політики, перетворюючи їх на практичні кроки, що забезпечують послідовність і точність виконання AML-стратегій.

Особливу увагу приділено інтеграції штучного інтелекту (AI) в AML-політики та процедури. AI допомагає виявляти нові ризики, забезпечує постійний моніторинг та покращує ефективність процесів. Наприклад, AI може аналізувати великі обсяги даних для виявлення підозрілих транзакцій, автоматизувати моніторинг і навчання співробітників, а також проводити аудити на відповідність політикам і зовнішнім регуляторним стандартам.

У дослідженні також наведені реальні приклади успішної інтеграції AI у фінансові установи, що значно покращили їхні AML-програми. Наприклад, великі фінансові інститути використовували AI для виявлення нетипових моделей транзакцій, що дозволило ефективніше реагувати на загрози.

Рекомендації для AML-фахівців включають регулярний перегляд та оновлення політик і процедур, інвестиції в AI і технології, проведення комплексного навчання співробітників та активну взаємодію з регуляторними змінами. Стаття підкреслює, що надійні AML-політики та процедури є основою для захисту цілісності фінансових систем і запобігання фінансовим злочинам.

https://fincrimeagent.com/aml-and-financial-crime-policies-and-procedures/

Звіт UIF Italy за 2023 рік вказує на зростання ромі мистецтва у відмиванні коштів

Звіт від Unità di Informazione Finanziaria (UIF) Італії за 2023 рік висвітлює важливі аспекти ролі мистецтва у боротьбі з відмиванням коштів та фінансуванням тероризму.

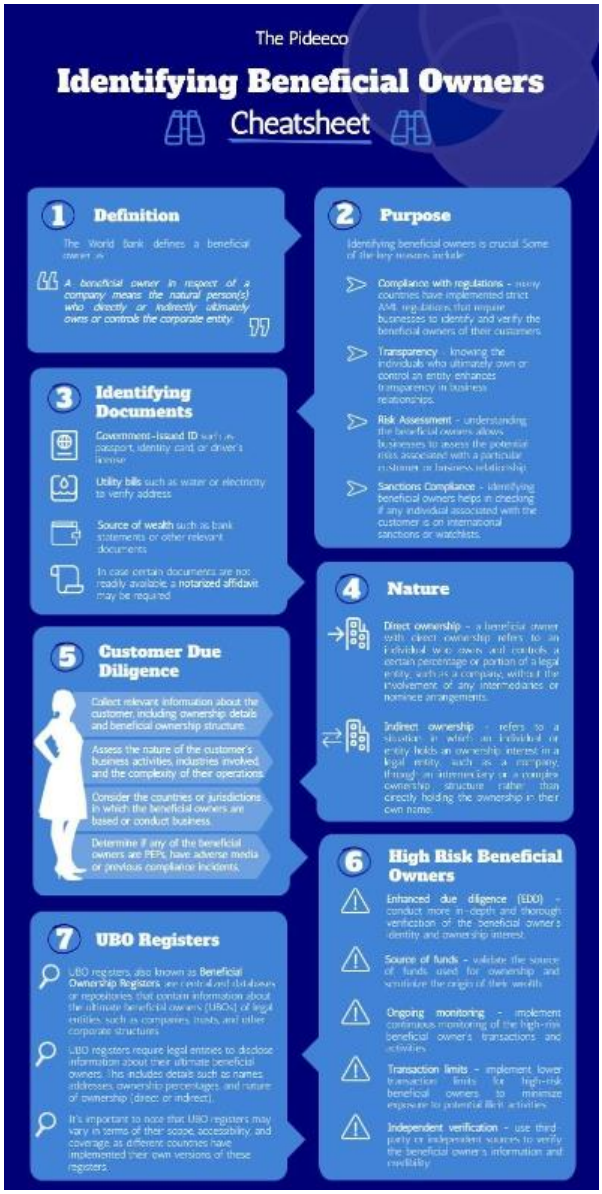
Основні моменти:

- Шахрайські схеми з мистетством: Мистецькі твори використовуються для обману інвесторів через фінансування покупок без належної перевірки документів. Кошти перераховуються продавцям, які згодом монетизують їх через зняття готівки та платежі в ігрових компаніях.
- Корупція в державному секторі: Виявлено випадки, коли чиновники отримували вигоди від переплат за мистецькі твори. Сектор мистецтва вважається ідеальним для відмивання грошей через високу вартість предметів, міжнародний характер ринку, використання посередників та офшорних структур, а також волатильність цін на мистецтво.
- Ризики, пов'язані з криптоактивами та NFT: Зростає використання криптовалют та NFT для ускладнення відстеження грошових переказів. У 2023 році кількість звітів про підозрілу діяльність від аукціонних будинків та художніх галерей зросла порівняно з 2022 роком, незважаючи на загальне зниження кількості таких звітів.

- Звіти від нефінансових операторів: UIF Italy зафіксувала 224 звіти від нефінансових операторів, що на 32,5% більше, ніж у 2022 році. Вони становлять лише 0,1% від загальної кількості звітів.
- Відновлення реєстру бенефіціарних власників: 19 вересня Рада проведе слухання щодо відновлення реєстру бенефіціарних власників, який вимагатиме від адміністраторів аукціонних будинків і галерей звітувати про бенефіціарних власників мистецьких творів та колекційних покупок у бізнес-реєстр.

https://bit.ly/3LiiHMs

Аналіз структури бенефіціарного володіння: думки і підходи



Важливість реєстру бенефіціарного володіння (BOR) на глобальному рівні зростає, оскільки він сприяє підвищенню прозорості та запобіганню фінансовим злочинам, таким як відмивання грошей.

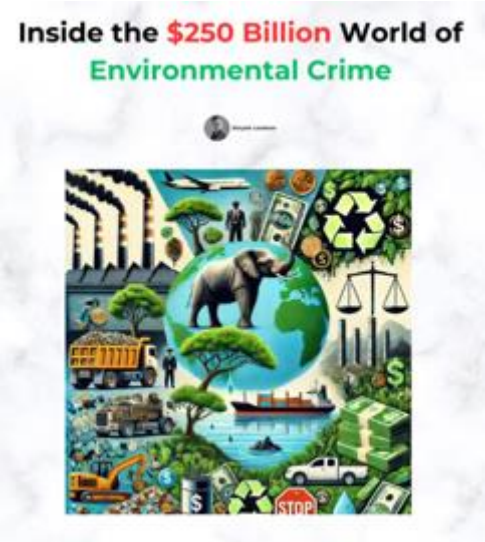
Існують різні підходи до доступу до цього реєстру. Деякі вважають, що відсутність реєстру підриває прозорість та створює умови для фінансових злочинів, і тому наголошують на необхідності відкритого публічного доступу. Інші підтримують обмежений доступ, який має бути відкритий лише для фінансових установ, регуляторів та слідчих органів, вважаючи, що такий підхід дозволить забезпечити належний контроль без надмірного втручання в приватність. Є також думка, що публічний доступ до реєстру може суперечити законам про конфіденційність і створювати ризики для власників бізнесу.

Ідентифікація бенефіціарних власників є важливим аспектом для забезпечення відповідності регулятивним вимогам, управління ризиками та запобігання фінансовим злочинам. Визначення бенефіціарного власника передбачає ідентифікацію особи, яка фактично контролює компанію. Для цього використовуються офіційні документи, такі як посвідчення особи, фінансові звіти та реєстраційні дані компанії. Належна перевірка клієнтів включає збирання та перевірку інформації про бенефіціарних власників.

Дебати щодо реєстрів бенефіціарних власників відображають баланс між необхідністю забезпечення прозорості для запобігання фінансовим злочинам і захистом прав на приватність. Вибір між відкритим доступом до реєстрів і обмеженням доступу до них тільки для уповноважених органів визначатиме майбутні стратегії боротьби з фінансовими злочинами на глобальному рівні.

https://bit.ly/4cSGu1e

Екологічні злочини: приховані загрози та їх зв'язок з відмиванням грошей



Екологічні злочини, також відомі як "зелені злочини", що включають незаконне вбивство тварин, контрабанду слонової кістки та рогів носорогів, незаконне виробництво відходів, забруднення, незаконний вилов риби та незаконну вирубку лісів, оцінюються приблизно в 250 мільярдів доларів. Ці злочини зростають на 5-7% щороку, що вдвічі перевищує темпи зростання глобальної економіки.

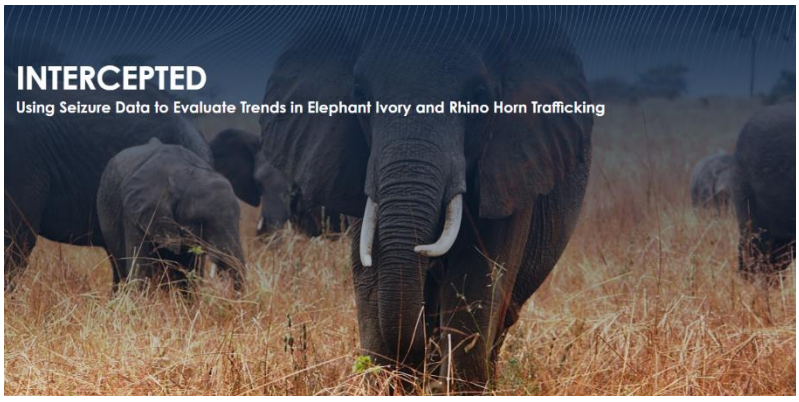
Основні причини, через які вчиняються екологічні злочини, включають їх високу прибутковість, оскільки, наприклад, злочини, пов'язані з дикою природою, приносять 23 мільярди доларів щорічно, що робить їх третьою за величиною фінансовою злочинністю за доходами. Крім того, багато країн мають недостатнє розуміння цих злочинів, що робить їх менш ризикованими у порівнянні з іншими незаконними діями. Великий попит на традиційну медицину та її нібито користь для здоров'я також сприяє поширенню цих злочинів. Зуби акул і роги носорогів використовуються для виготовлення фальшивих мазей та інших неліцензійних засобів нетрадиційної медицини.

Екологічні злочини часто пов'язані з відмиванням грошей, де злочинці використовують легальні бізнеси для приховування своїх незаконних дій. Фінансові установи можуть допомогти в припиненні цих транзакцій, але для цього їм потрібно бути уважними до ознак, таких як підозрілі компанії, нерегулярна діяльність, великі готівкові депозити або зняття коштів з різних країн та неповна інформація про клієнтів на митних або транспортних документах.

Загалом, екологічні злочини не тільки шкодять навколишньому середовищу, але й підривають правосуддя, справедливість та захист майбутніх поколінь. Вони є серйозною загрозою, що потребує спільних зусиль для боротьби з ними.

https://bit.ly/3LihODx

Аналіз тенденцій та Моделей незаконної торгівлі слоновою кісткою та рогами носорогів



Звіт "Intercepted" від C4ADS детально аналізує незаконну торгівлю слоновою кісткою та рогами носорогів, виявляючи нові тенденції та моделі в цій сфері після пандемії COVID-19. Основні маршрути торгівлі все ще проходять з Африки до Азії, з ключовими центрами в Південній Африці та В'єтнамі. Звітується, що вилучення слонової кістки зросли з 2021 року, тоді як вилучення рогів носорогів залишалися нестабільними, що вказує на адаптацію злочинних мереж до нових викликів.

Звіт підкреслює важливість міжнародної співпраці для боротьби з цією проблемою, а також акцентує на необхідності вдосконалення технологій моніторингу та контролю на митницях. Автори

закликають до посилення правового переслідування та збільшення ресурсів для правоохоронних органів, щоб ефективніше боротися з цією глобальною загрозою.

Рекомендації звіту включають покращення обміну інформацією між країнами, впровадження нових технологічних рішень для відстеження контрабанди та підвищення рівня освіченості населення щодо наслідків незаконної торгівлі дикою природою. Документ також зазначає, що зменшення попиту на продукти з дикої природи в країнах-споживачах є критичним для скорочення обсягів торгівлі.

https://c4ads.org/reports/intercepted/

Telegram + TON: Ідеальне поєднання для шахраїв?

Стаття попереджає про серйозні ризики шахрайства, пов'язані з використанням Telegram та його цифрового активу TON (The Open Network). Telegram, з більш ніж 900 мільйонами користувачів, відомий своєю конфіденційністю та шифруванням, що ускладнює правоохоронним органам відстеження шахраїв. Ця платформа з обмеженим зберіганням даних та розподіленими операціями потрапляє у "сіру зону" законодавства, що ускладнює фінансові розслідування.

Проблема ускладнюється можливістю екстремальної анонімності: зашифровані чати та криптовалютні транзакції створюють подвійний рівень непрозорості, який шахраї можуть використовувати для своїх схем. Швидке поширення шахрайств стає можливим завдяки глобальній базі користувачів Telegram, де шахрайські схеми можуть розгортатися дуже швидко. Боти Telegram можуть бути запрограмовані на автоматичне виконання криптовалютних шахрайств у великому масштабі, що робить ці платформи привабливими для шахраїв.

Маніпуляції на ринку також є значною загрозою, оскільки близькі спільноти можуть легко розгорнути схеми "pump-and-dump". Telegram полегшує створення підроблених облікових записів, що сприяє крадіжці особистих даних та інших видів шахрайства. Децентралізований характер TON приваблює тих, хто хоче обійти фінансовий нагляд, що робить систему вразливою до шахрайських дій.

Особливо стурбованість викликає розширення мережі Tether на платформу TON, що додає додаткові ризики фінансового шахрайства. Стаття закликає користувачів бути надзвичайно обережними з "занадто гарними, щоб бути правдою" пропозиціями та ніколи не ділитися конфіденційною інформацією через месенджери.

http://surl.li/mujkre

Оновлення списку високо-ризикових країн FATF

FATF опублікувала оновлений список високо-ризикових країн станом на 1 липня 2024 року для цілей боротьби з відмиванням грошей та фінансуванням тероризму. Зі списку країн під посиленим моніторингом (Grey List) були виключені Ямайка та Туреччина, а додані Монако та Венесуела. Незважаючи на видалення з списку FATF, Ямайка залишається країною високого ризику відповідно до класифікації ЄС. Це рішення засноване на оцінках ризиків, проведених FATF та Європейською Комісією, які враховують різні фактори, включаючи ефективність боротьби з відмиванням грошей та фінансуванням тероризму у цих країнах. Важливо відзначити, що статус країни у списку може мати значний вплив на її фінансову та економічну стабільність, оскільки він впливає на міжнародні фінансові операції та інвестиції.

http://surl.li/esirzu